Below are several interesting pieces of e-news. My thanks to all who contributed info.
Have a great weekend!!!
Ken

COVERED ENTITY AND IMPACT / CHANGE TO PROCESSES:
Per Tom Hanks, an authority on HIPAA, a key point in determining if you are a "covered entity" is: 1) If a provider conducts electronic transactions, they are a covered entity and all PHI maintained by them in any form is covered under the Privacy rule, including information printed. and, 2) If they do not conduct electronic transactions, nothing they do is covered under HIPAA, including what they print.

My personal caution is that we must consider that even if you are not a cover entity, you may be impacted by HIPAA if your business partners, providers or those collecting / passing data to you do convert to HIPAA conventions. If they use code sets and formats that do not reflect your current processes then you may be impacted. Data collected in HIPAA conventions may not reflect the information you expect related to demographic information, diagnosis, provider information, drug codes, error codes, etc. An example: HIPAA at this time has only 8 race/ethnicity codes and some systems now use and report up to 58 codes. Just a thought.....

TOPICS INCLUDED BELOW:

********** [hipaalive] RE: "Covered entity" **********
>>> tom.hanks@beaconpartners.com 04/05/01 12:38PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

1) If a provider conducts electronic transactions, they are a covered entity and all PHI maintained by them in any form is covered under the Privacy rule, including information printed.
2) If they do not conduct electronic transactions, nothing they do is covered under HIPAA, including what they print.

Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.

********** [hipaalive] Cost Of Implementing HIPAA **********
*** This is HIPAAlive! From Phoenix Health Systems ***

Fellow HIPAAlive Members:

Has anyone reasonably and with sufficient thought calculated out what they think the total cost of implementing HIPAA requirements in their present form (finalized or not) might be for their particular healthcare location? Please reply only if you're a healthcare provider, which is a hospital or hospital system. Please include appropriate information so that a comparison can be drawn.

For example, single hospital (educational & research institute, providing primary, secondary & tertiary pediatric patient care) with 300 beds, 5500 employees, $505 million in total revenue this year, spending an identified $5.4 million on its HIPAA initiatives over the next 2 years. Already spent $.25 million in current fiscal year for assessment study and related miscellaneous items.

Anyone out there able to provide such benchmark information? Thanks.

-J. Eric Stevens

********** [hipaalive] Study: HIPAA Data Standards Costs Underestimated **********
>>> cjackson@mcare.med.umich.edu 04/04/01 05:23AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***
Another member of the group forwarded this link to the report itself -- the report has the date for transactions noted correctly. Seems as though Health Data Management noted it incorrectly or mistakenly noted the compliance date for small plans.
http://bcbshealthissues.com/relatives/17841.pdf
Cathy Jackson
Privacy and Security Project Manager
M-CARE
Ann Arbor, Michigan

>>> aseltzer@healthtek.com 04/03/01 01:46PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***
Here is the link for the article:
http://www.healthdatamanagement.com/html/hipaa/NewsStory.cfm?DID=5262

**** [hipaalive] CODE SETS - Further Clarification on BIPA Extension for Select Local Codes ********
>>> ApgarC@providence.org 04/04/01 09:26AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

FYI - The following is from HCFA and further explains what is and isn't covered under the local code set extension included in BIPA.

Chris Apgar,
Data Security & HIPAA Compliance Officer
Providence Health Plan
Phone: (503) 574-7927, X-47927
Fax: (503) 574-8655
Pager: (800) 425-5123
E-mail: apgarc@providence.org <mailto:apgarc@providence.org>
Pager E-mail: 4255123@archwireless.net
<mailto:4255123@archwireless.net>

Don't Bet On BIPA...
BIPA Does Not Keep Medicaid Local Codes Alive
Another Year

The Medicare, Medicaid, and SCHIP Benefits Improvement and Protection Act of 2000 (BIPA) (Public Law Number 106-554) was signed into law on Thursday, December 21, 2000. Many erroneously believed it stated that Medicaid local codes would be extended one additional year after the implementation of the transaction rule:

"Section 532 Retention of HCPCS Level III Codes:
(a) In General _ The Secretary of Health and Human Services shall maintain and continue the use of level III codes of the HCPCS coding system (as such system was in effect on August 16, 2000) through December 31, 2003, and shall make such codes available to the public.
(b) Definition _ For purposes of this section, the term "HCPCS Level III codes" means the alphanumeric codes for local use under the Health Care Financing Administration Common Procedure Coding System (HCPCS)."

Medicare recently issued instructions to its Fiscal Intermediaries and Carriers explaining that, under the BIPA, HCPCS Level III codes have been granted an extension and are to be accepted through December 31, 2003. This has led to renewed confusion as to whether Medicaid local codes are included.

By and large, Medicaid local codes are not Level III

HCPCS codes as defined by BIPA. Level III HCPCS codes are those submitted through HCFA regional offices for approval by the HCFA HCPCS code committee as Level III local codes. Most Medicaid Agencies did not submit their local codes to the committee. Likewise, most codes developed by States, private payers, the Department of Veterans Affairs, Department of Defense, and others are NOT Level III codes. States Agencies should notify providers to plan to comply with national HCPCS codes by the October 2002 date.

Medicare carriers and intermediaries did submit codes for official Level III approval, in order to be able to use them for Medicare purposes, but even Medicare has been phasing out this method of assigning codes. They have replaced it with the Level II application process that the NMEH local code effort is using. There are very few Level III codes in existence at this point, because the phase out is almost complete. For a list of codes that can be used, please contact the Medicare Fiscal Intermediaries and Carrier(s) and Durable Medical Equipment Carriers (DMERCS) for your state.

********** [hipaalive] RE: FW: PRIVACY - New Congressional bill **********

>>> tom.hanks@beaconpartners.com 04/02/01 01:22PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

The problem is the current HIPAA legislation does not give HHS the authority the address patient information in the same way as the Greenwood bill. That lack of authority is what created the Business Associate Contract and the inability to supercede state law.

Thanks,

Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.
Hoffman Estates, IL 60195
PH: 847.490.5306
Email: tom.hanks@beaconpartners.com

CONFIDENTIALITY NOTICE: This e-mail communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. If you are not the intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited. If you have received this communication in error, please notify Beacon Partners immediately by telephone at (781) 982-8400, x225 and destroy all copies of this communication and any

attachments.

-----Original Message-----
From: Mic Sager [mailto:MSager@olympicmedical.org]
Sent: Friday, March 30, 2001 12:42 PM
To: HIPAAlive Discussion List
Subject: [hipaalive] RE: FW: PRIVACY - New Congressional bill

*** This is HIPAAlive! From Phoenix Health Systems ***

I agree Bill. What I was thinking is this may be a "template" for a republican administration to re-write the rule. Any thoughts? - Mic

********** AHIMA ADVANTAGE E-ALERT Volume 3, Issue 7 **********

AHIMA ADVANTAGE E-ALERT
Volume 3, Issue 7

AHIMA SUBMITS COMMENTS ON HIPAA PRIVACY RULE

AHIMA has responded to HHS Secretary Tommy Thompson's request for technical
comments on the Final HIPAA Privacy Rule in a recent letter. In the comments, the Association urged Thompson to move forward with the HIPAA Privacy Rule.

"AHIMA reiterated its desire to see the Final Privacy Rule take effect April 14, 2001," stated AHIMA's executive vice president and CEO, Linda Kloss, MA, RHIA. "This Rule is about balancing the individual's right to privacy with the healthcare industry's need for critical information to deliver service and operate a complex system. The learning won't happen overnight and the Rule must evolve as learning takes place. In the meantime, there are technical changes that can be made within the context of HIPAA which will clarify certain provisions and streamline others."

AHIMA also issued comments with the Association's alliance partners, the Coalition for Health Information Policy (CHIP). Members of CHIP include AHIMA, the American Medical Informatics Association (AMIA), the Center for Health Information Management (CHIM), and the Healthcare Information and Management Systems Society (HIMSS).

For a complete copy of AHIMA's letter, visit the Association's Web site at http://www.ahima.org/dc/thompsonletter.htm.

NEW HIPAA DISCUSSION FORUM ON AHIMA'S PRACTICE FORUMS

If you're interested in discussing the HIPAA Privacy Rule, have questions about how redisclosure of health information received from other healthcare providers changes under HIPAA, how to deal with patient requests to review and amend their records, or other questions related to HIPAA, there's now a new Practice Forum for you! AHIMA's HIPAA forum gives members a place to ask questions, share plans and ideas, and just find out how other members are dealing with the sweeping changes mandated through HIPAA. Visit the forum today at http://www.ahima.org/bbs2-bin-hpf/bbs-31/open_forum?31+0.

JUST ADDED--NEW HIPAA AUDIO SEMINARS

Join our experts as they bring you the latest, most comprehensive information on HIPAA. In four information-packed audio seminars, you'll get the facts you need to ensure compliance and your understanding of this far-reaching legislation:

Positioning the Privacy Officer, Wednesday, April 25
Business Partner Agreement, Tuesday, May 8
Notice of Privacy Practices, Tuesday, June 5
Preemption and State Laws, Tuesday, June 12

Attendees earn AHIMA CE credits. Plus, after each seminar, attendees will have access to a week-long Web forum. Only audio seminar attendees will have access to these forums, and there is no extra charge. The registration deadline is three business days before the seminar date. Access is limited, so register today! For registration and more information on these and other AHIMA audio seminars, visit http://www.ahima.org/products/seminars.html.

Seminars last 90-minutes beginning at 1 p.m. ET, 12 Noon CT, 11 a.m. MT, and 10 a.m. PT. The cost is $135 for each seminar, or four seminars for $486.

Also, on Tuesday, April 10 at 1 p.m. E.T., AHIMA is joining forces with St. Anthony Publishing to bring you the audio seminar, HIPAA Privacy Regulations in the Acute Care Setting. This seminar will give you a clear understanding of the privacy requirements and how they will impact your acute care facility (small-medium hospitals). St. Anthony Publishing is handling registration, and AHIMA members receive a $50 discount off the regular price of $199.95. For more information and registration, call toll-free, 1-800-632-0123.

********** [hipaalive] RE: Remote Printing **********
>>> tom.hanks@beaconpartners.com 04/02/01 01:12PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Gwen,

Remote printing has some of the same issues as faxing.

1) You should ensure that the parties for whom the print job is being produced are authorized to have access to the information being printed and that only those parties have access to the printed documents.
2) Also, you should have a retention and destruction policy for all printed information. E.g. at the end of the day, any printed information contained PHI should either be shredded or placed in a secure area (e.g. locked file cabinet).

Thanks,

Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.
Hoffman Estates, IL 60195
PH: 847.490.5306
Email: tom.hanks@beaconpartners.com

CONFIDENTIALITY NOTICE: This e-mail communication and any attachments may
contain confidential and privileged information for the use of the designated recipients named above. If you are not the intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited. If you have received this communication in error, please notify Beacon Partners immediately by telephone at (781) 982-8400, x225 and destroy all copies of this communication and any attachments.

********** [hipaalive] Remote Printing - independent medical transcriptionist **********
Tom Hanks wrote:
> *** This is HIPAAlive! From Phoenix Health Systems ***
> Phyllis,
> >From your response, it appears that you are an independent medical
> transcriptionist. As such you would not be considered a covered entity

> under HIPAA. However, you would be controlled by your customer's Business
> Associate Contract. If you abide by their contract, then the burden is on
> your customer to specify where you fax or print the information. It is then
> up to them to ensure that the information is safeguarded and protected at
> those specified locations. It may be helpful for your customers if you
> suggested some language that specified where you were fax and/or print
> information and stipulated that only personnel authorized to receive the
> information had access to those faxes/printers.
>
> I hope this helps,
>

********** [hipaalive] PRIVACY:Clinical Document Delivery Options **********
>>> dhf@faxnet.com 04/05/01 06:32AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

It has been very interesting watching this list regarding the delivery of medical information and documents to remote locations via various methods. All the discussed methods have the same problem of verification of the actual person receiving the information.

FAX - The hospital sends to a phone number that is associated with a practice. Yes, it is possible to have protected phone lines from the phone companies. With FAX we do not know who actually received the documents in the physician's office, just that it was received. (Note many Windows based faxing packages/servers do not really know that the documents was actually sent properly. A good fax server will follow the CITT standard to the letter in the conformation of receipt. This type of server may duplicate copies because of line noise, but we are sure the documents were received.) An office staff member or other physician may pick up the documents for the fax machine.

Much of this can be handled via written procedures and protocols the practice agreed to when they requested to receive documents via FAX such as where the FAX machine is placed, and who has access to the machine.

E-MAIL - E-mail can be directed to a particular physician in a practice and be encrypted in transit. But as we all know, most physicians do not want to handle the number of reports being delivered to them from the hospital. The more time they spend opening e-mail, the less time they have to see patients. They usually have their office staff print the documents and in many cases they actually do not read the information if the results are normal. Again the hospital does not know who actually received the documents and once they are printed, just as in the case of FAX, the document is visable to anyone while it is sitting on the printer on somewhere else.

Again, we still need to have written procedures and protocals in place for the practice to receive documents via e-mail. We have gained nothing over the simplest method of document delivery - FAX.

US Mail - As we all know mail is sometimes missed delivered and opened by accident especially if the hospital uses their address only without their name as was suggested in this list. The wrong person just saw protected patient informaiton. If the letter was delivered the proper practice, it is probably opened by some receptionist while he/she is waiting on other patients. A person looking over the counter could easily see protected patient information. The hospital does not know to whom the documents were actually delivered. All they know is that they placed the letter in the US mail. There is no guarantee that it got to the correct place nor who at the practice received it. I guess they could use certified addressee only.

Again, there still needs to be written procedures and protocals in place for the practice to receive documents via the US mail. The US mail may actually be the least secure delivery method.

The only secure method of document delivery is to physically hand the documents to the physicians while they are in the hospital and make them sign for a proof of delivery. This way the hospital knows who actually received the information. But, again as we know documents given to or picked up by physicians do not always reach their office.

Given the above it seems that the only way to get the information into the physician's hand is to establish a secure web site for them to go, login with biometric authentication and view/print the document from there. In this case we know who actually view or had access the documents. If they print them in their office, the hospital can not control that. The printed version should contain some indication that states the document was printed for a particular user/physician.

There is still a problem with this method. The physician could login and have the office staff view or print the the documents.

I guess the only way to be sure of who see and has access to the patient's record is to require that the physician only look at the hospital reports while in the hospital and sign that each report was looked at.

Donald French
dhf@QuickChart.com
VertiSoft

********** New England Health EDI Network Case Study **********

For an interesting case study on implementation of HIPAA, the web site www.nehen.net/casestudy.htm has an interesting article.